Recorded Future®

SOAR
SOLUTION
OVERVIEW

Splunk SOAR: Recorded Future Threat Hunting Playbook

Use Case

After a Splunk SOAR container is created it will be populated with artifacts which can then be enriched with threat intelligence. Recorded Future provides technical links which are verified relationships between indicators of compromise provided by enriched entities. These technical links will help analysts find new intelligence relevant to their organization and make quick decisions based on the verified data.

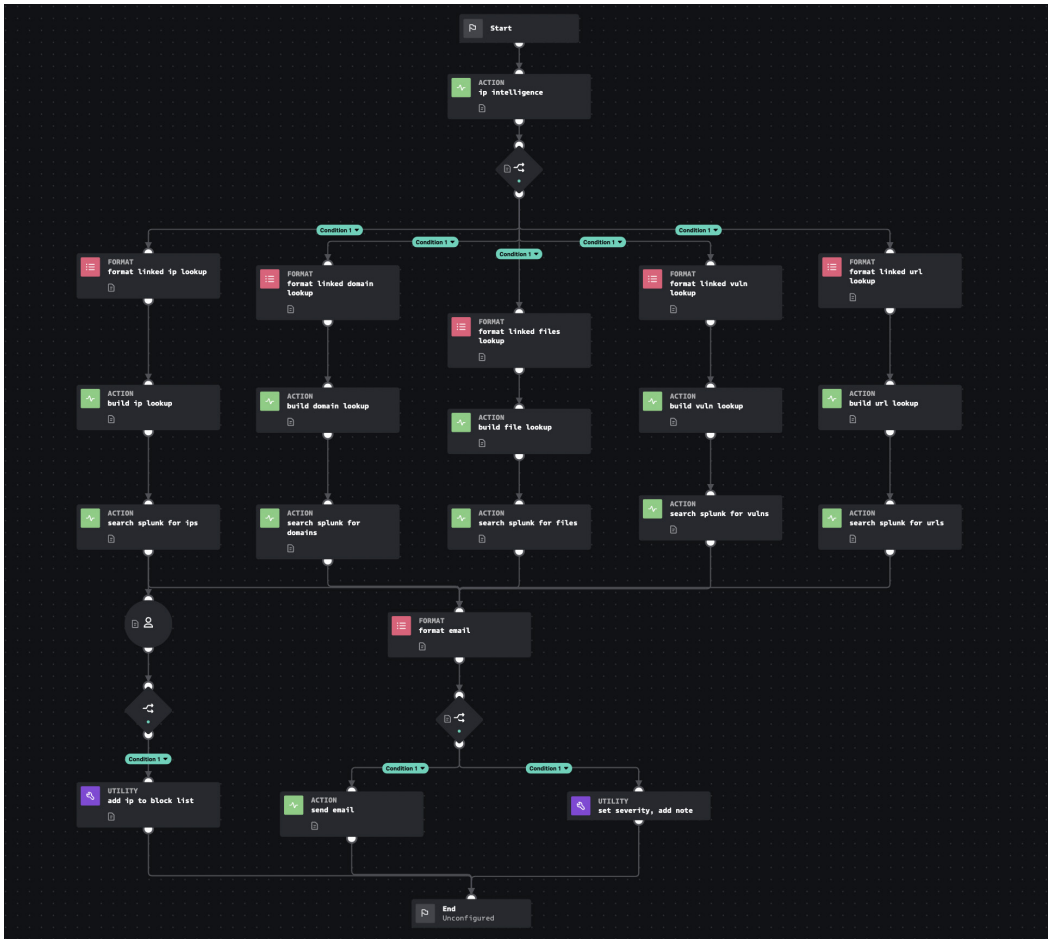
For example, a malicious IP address can have a verified link to several domains or hashes. These links should be searched across a company's network but this can be a time consuming task. This playbook will enrich all artifacts containing IP addresses, check for verified links, and search Splunk for any matches.

Issue

Manual cycle time required to investigate links between indicators of compromise by performing threat hunting searches within Splunk Enterprise.

Solution

Starting with a single IP address, this playbook gathers a list of linked IP addresses, domain names, file hashes, URLs, and vulnerability CVEs from Recorded Future. Then, Splunk is used to build threat hunting lookup tables and search across multiple data sources for events containing the linked entities. Finally, IP addresses are blocked if approved by an analyst and an email is sent to notify a responder of the activity.



Technical

From a technical perspective the integration will include and need configured:

- Splunk SOAR connectivity and read permissions from Splunk Enterprise
- The Recorded Future app for Splunk SOAR installed and configured **https://splunkbase.splunk.com/app/6050**

This service will require the SecOps or Threat Intelligence Module and the Recorded Future Splunk SOAR Integration. The playbook will be included with the Recorded Future App on the Splunk SOAR marketplace.